

The Hidden Costs of Not Planning for Disasters



By [Leo Wrobel](#), [Sharon Wrobel](#)

Date: May 12, 2009

[Return to the article](#)

During these trying financial times, are you having trouble obtaining money for your disaster recovery plan? It might be high time to refine your approach. Leo A. Wrobel and Sharon M. Wrobel, specialists in disaster recovery and business resumption planning, explain how to help your executives focus on the true costs involved in failing to plan.

In this article, we'll share with you some scary stories about big checks that some companies have had to write, due to lack of adequate planning. We've highlighted important ideas to emphasize when presenting your case with executives: that *disaster recovery planning makes a lot of sense*.

What facts are considered the most relevant and important to upper management? You may recall from our previous articles that, fundamentally, management needs to know only *four things* in order to decide whether to fund your plan:

- What *can* happen? (Fire, flood, hurricane, sabotage, etc.)
- What is the *probability* that it will happen? (Expressed best in percent probability of the event in a given year.)
- What does it *cost* when it happens? (Expressed in terms of lost sales, market share, employee productivity, and customer confidence.)
- What does *preventing* it cost? (Expressed as a high-level overview of the proposed protective system procedure, or function.)

Loss of Customer Confidence

Let's do some thinking about cost but with a twist. "Cost" is not always limited to money for rebuilding buildings and systems. Indeed, your business may experience *indirect* costs that are not even financial at first, anyway. Consider this scenario: If a distraught parent can't get through to a 911 call center after little Johnny swallows drain cleaner, a real tangible cost is involved. Everyone concerned ends up on the news (and not in a good way), and someone's job is most likely on the line and don't forget the possibility of legal repercussions. Now think about some of the other potential costs outlined in the following real examples:

Consider the letter I received from my bank recently. You can see the full document in [Figure 1](#), but I'll cut to the chase for you:

[W]e believe one of our most important jobs is to provide the highest possible level of security for our customers. And that is the purpose of this letter. Visa recently notified us that some of our customers [sic] debit card numbers[...] may have been stolen when a third-party vendor's systems were compromised. Upon receiving this information, we immediately took the necessary action to protect you from any potential threat.

Uh, oh. This doesn't sound good. The letter goes on:

As a result, you will soon be receiving a new check card with a new number that will replace your existing card. Your new card should arrive within the next 7 to 10 days.



Figure 1

Oh, rats. Do these people realize how many places (car rental companies, airlines, and so on) now have to be changed for my "new" card?! This is one of those hidden costs: *customer confidence*. A bit later on, the letter continues with even more good news

Your existing card number will be deactivated automatically within 30 days and will no longer be available for you to use

This little present from my bank promises to become the gift that keeps on giving: Months from now, when I travel rental car companies and airlines will be calling me because the numbers in my "secret profile" with them no longer work.

Accidents happen—that's why you plan! But this isn't Visa's first accident. A few years back, one of Visa's servers was stolen, with several hundred thousand credit card numbers on it, and customers and clients went through the same trauma that time around

Consider the letter I received from the U.S. Veterans Administration a couple of years ago. A laptop was ripped off, and it contained Social Security numbers and other personal info for *millions* of veterans. I'm concerned; I used to be Sergeant Wrobel. Again, not only the cost of the equipment was a factor, but also the bad faith associated with the loss.

And the problem isn't getting any better

Do you have an iPhone or a BlackBerry? The phone I carry has 16GB of memory. I make it a point *not* to carry critical data on my phone, although it does have a lot of people's email addresses and phone numbers.

Can you just imagine if the CEO of one of today's financially strapped automakers, banks, or some other company dropped his or her PDA in the Dallas/Fort Worth airport, and that little gadget fell into the wrong hands? Can you picture the people who could suddenly be short-selling the stock of that corporation? Two lessons to learn here:

- The obvious lesson is the cost to your company if this sort of accident happens
- The less-obvious lesson is that wireless technology such as iPhones and BlackBerry devices takes data which used to be very secure in computer rooms or server closets and, for better or worse, transfers it to people's pockets. Have you updated your security standards to include PDAs?

Penalties and Lawsuits

Here's another way you can lose by not planning for disasters: contractual and nonperformance penalties. One of the biggest companies in America, Dallas-based AT&T, is learning this lesson the hard way, according to an article in Exchange Magazine. AT&T had a computer room disaster (caused by a water main break) that affected its wholesale customers, and AT&T's contracts with those customers contain *performance measure* (PM) provisions. If performance to wholesale customers degrades, AT&T owes those customers a lot of money under their contracts. In this case, that amount is potentially enough to get AT&T's legal staff involved. The AT&T lawyers are claiming that the contracts are not valid in this particular case. Their reason? God did it. This phenomenon is known in the legal world as a *force majeure* event. AT&T is claiming *force majeure* in an attempt to dodge contractual penalties for the disaster. We submit that some disaster planning would have been cheaper. Read on

A trade association called CompSouth (which represents AT&T competitors) is calling on state commissions to reject AT&T's *force majeure* claim, since if approved by regulators it would allow AT&T to avoid its contractually mandated

performance-remedy payments to CLECs in nine states. Indeed, AT&T filed a notice that the disaster a flood and subsequent power outage in its St. Louis data center in December qualifies an act of God. Therefore, AT&T says, it doesn't owe CLEC customers for downtime they suffered as a result

AT&T has a long history of trying to dodge performance payments to its competitors (Take a look at our Dallas-based TellLawCom Labs Inc. website for one example.) Setting this issue aside, however, the disaster AT&T is depending on to avoid penalties was preventable by any standard: On December 6, 2008, the basement of AT&T's St. Louis data center flooded because of a water main break. A power outage followed. So what's wrong with this picture? What's wrong is that serious contingency planners have been mediating concerns like water and power outages since Fred Flintstone bought his first stone PC. If you don't believe me, check out my 1993 book *Writing Disaster Recovery Plans for Telecommunications Networks and LANS* (Artech House Books). Virtually all of Chapter 5 discusses these very issues, complete with pictures and diagrams (see Figure 2) advising planners to install drains, place equipment away from sources of water, install uninterruptible power systems, and other standards and practices long since adopted by serious contingency planners. That's 1993, people more than a decade and a half ago!

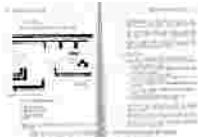


Figure 2 Reprinted with permission by Artech House Books

By all indications, the AT&T issue will be settled in the courts or regulatory commissions. And AT&T's wholesale customers believe that the contract is in their favor. For example, AT&T didn't declare the event an act of God until February 10, 2009, despite obligations to do so right away. AT&T did tell its CLEC customers that the flood and outage had occurred, but waited two months to dub the incident an official *force majeure* in state commission filings. Perhaps that's how long it took for AT&T management to realize how much money was at the line?

"Not so fast," say AT&T's competitors. Under agreements between AT&T and CompSouth's 12 members, AT&T must promptly notify several entities of a *force majeure* event. AT&T is supposed to maintain certain operational support systems (OSS) performance metrics for its wholesale users or pay up, unless the interruptions stem from an unforeseen act of God. To that end, AT&T said in February that the December flood was indeed a *force majeure*, and the company shouldn't have to compensate CLECs in nine states for the December 2008 outages. CompSouth vehemently disagrees, and we vote with CompSouth.

A water main break is preventable, and standards for water damage in equipment areas have been established for 25 years or more. There is simply no excuse for something like this to happen. CompSouth argued in a February 11 filing with the Florida Public Service Commission that AT&T followed improper procedures in dealing with the flood and did not have backup redundancy in the data center, as it should have. This kind of issue is the contingency planner's worst nightmare.

Summary

We hope that this article has tuned you in on the benefits of proactive planning, including the avoidance of indirect costs should a mishap befall your organization. Often, the costs you don't consider in advance turn out to be the highest of all. Don't be a headline—review your procedures today. Until next time, best of luck in your endeavors, and happy planning.

In addition to his work with his own two companies, TellLawCom Labs Inc. and b4Ci, Inc., Leo A. Wrobel is honored to have been elected president of the Networking and Systems Professionals Association (NaSPA), a not-for-profit company concentrating on the needs of tens of thousands of members since 1986. NaSPA specializes in career development, employment, information technology, and disaster recovery. Contact Leo at 214-888-1300 or email leo@b4ci.com.

Sharon M. (Ford) Wrobel served as corporate secretary and director of personnel for Premiere Network Services Inc. prior to joining b4Ci, Inc. in 2004. During that time, Sharon was instrumental in getting Premiere certified as the first CLEC to be certified in all 50 states, by aiding in filings and attending hearings. She also engaged in extensive research for Premiere, a function she continues with b4Ci as vice president of business development.

Sharon was also president of the Ellis County Early Childhood PTA and the Ovilla Lions Club. She attended the University of Maryland and El Centro College in Dallas and received training as a registered nurse before joining Leo in business in the late 1990s. Sharon also served as a public official by accepting appointments to the local Planning and Zoning Commission and the Historical Commission.
